暗号理論 (B1)
最終レポート

山下 恭平
学籍番号:2600200443-6

2023 年 1 月 19 日

1 AES(Advanced Encryption Standard)

1.1 共通鍵暗号/AES

AES とは「Advanced Encryption Standard」の略であり共通鍵暗号の一種である．AES は Daemen と Rijimen の提案した Rijndael という暗号化アルゴリズムを基に開発された.

1.2 Rijndael

1.3 title

RC4:1987 年に開発、アルゴリズムは非公開であったが 1994 年に何者かによって漏洩させられ,2015 年 2 月には TLS のすべてのバージョンにおいて RC4 の利用を禁止する提議 RFC 7465 [1] が公開された.

アメリカ国立標準技術研究所 (NIST)

2 TLS

2.1 TLS とは

2.2 title

2.3 title

参考文献

[1] A complete guide to the common vulnerability scoring system. `https://www.rfc-editor.org/rfc/rfc7465` . (15/12/2022)

[2] Octavian Suciu , Connor Nelson , Zhuoer Lyu , Tiffany Bao , and Tudor Dumitras. Expected Exploitability: Predicting the Development of Functional Vulnerability Exploits. In 31th USENIX Security Symposium (USENIX Security 22), pages 377-394, 2022